CLAIMS

    1.   A method of securing access to resources in a computing device, comprising the steps of:

    storing an encrypted access code in a known memory location with the

5   computing device;

    receiving a password to access the resources;

    encrypting the password to produce a encrypted password;

    comparing the encrypted password to the encrypted access code;

    allowing access to the resources if the encrypted access code matches the

10   encrypted password.

    2.   The method of claim 1 wherein the step of storing an encrypted access code comprises the step of storing a hashed access code.

    3.   The method of claim 2 wherein the step of encrypting a password comprises the step of hashing a password.

15   4.   The method of claim 1 wherein the encrypted access code is stored in a memory that cannot be externally modified.

    5.   The method of claim 1 wherein the step of allowing access comprises the step of allowing access to testing resources if the encrypted access code matches the encrypted password.

20   6.   The method of claim 1 wherein the step of allowing access comprises the step of allowing access to change system parameters if the encrypted access code matches the encrypted password.

    7.   A computing device comprising:

    a processing system

25   a memory for storing an encrypted access code;

input circuitry for receiving a password to access the resources;

wherein the processing circuitry:

encrypts the password to produce a encrypted password;

compares the encrypted password to the encrypted access code;

5   allows access to the resources if the encrypted access code matches the encrypted password.

8.   The computing device of claim 7 wherein the encrypted access code comprises a hashed access code.

9.   The computing device of claim 8 wherein the encrypted password

10   comprises a hashed password.

10.   The computing device of claim 7 wherein the encrypted access code is stored in a memory that cannot be externally modified.

11.   The computing device of claim 7 wherein the processing system allows access to testing resources if the encrypted access code matches the

15   encrypted password.

12.   The computing device of claim 7 wherein the processing system allows access to system parameters if the encrypted access code matches the encrypted password.